UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to CONSUMER Cases

CAPITAL ONE DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

KING & SPALDING LLP

David L. Balser (*pro hac vice*)
S. Stewart Haskins II (*pro hac vice*)
Susan M. Clare (*pro hac vice*)
John C. Toro (*pro hac vice*)
Kevin J. O'Brien (VSB No. 78886)
Robert D. Griest (*pro hac vice*)
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
sclare@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

TROUTMAN PEPPER HAMILTON SANDERS LLP

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
1001 Haxall Point
Richmond, VA 23219
Tel.: (804) 697-1200
Fax: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
S. Mohsin Reza (VSB No. 75347)
401 9th Street, NW, Suite 1000
Washington, DC 20004
Tel.: (202) 274-1932
Fax: (202) 274-2994
mary.zinsner@troutman.com
mohsin.reza@troutman.com

Counsel for Capital One Defendants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

EXHIBITS

EXHIBIT LETTER	DESCRIPTION
A	Plaintiff Brandi Edmondson's HSBC credit card statements, CAPITALONE_MDL002204932
B	Compilation of 48 Member Plaintiff fact sheets showing prior data breaches
C	Exemplar mail solicitations, CAPITALONE_MDL_00238124 CAPITALONE_MDL_002843767, and CAPITALONE_MDL_002844275
D	Capital One web application interface for various credit card types 2017-2019, CAPITALONE_MDL_00211429
E	Capital One's Supplemental Responses to Interrog. Nos. 10, 11, 13 and 14
F	July 28, 2019 Capital One Internal Memo regarding Likelihood of Dissemination, CAPITALONE_MDL_001206466
G	Expert Rebuttal Report of Art Ehuan
H	Expert Report of Lorin M. Hitt, Ph.D.
I	Expert Report of Rebecca E. Kuehn
J	K2 Integrity personal information report regarding Plaintiff Caralyn Tada, CAPITALONE_MDL_002857248
K	September 1, 2020 Facebook post by Caralyn Tada, *available at* https://www.facebook.com/photo?fbid=10224242287231438&set=gm.2673640592963784 (last visited May 26, 2021).
L	K2 Integrity personal information report regarding Plaintiff Emily Behar, CAPITALONE_MDL_002857253
M	K2 Integrity personal information report regarding Plaintiff Brandi Edmondson, CAPITALONE_MDL_002857235
N	K2 Integrity personal information report regarding Plaintiff Emily Gershen, CAPITALONE_MDL_002857260
O	K2 Integrity personal information report regarding Plaintiff Sara Sharp, CAPITALONE_MDL_002857280
P	Compilation of 19 Member Plaintiff fact sheets showing identity theft and fraud prior to March 2019
Q	Expert Rebuttal Report of Kevin Mitnick
R	Expert Rebuttal Report of Gary Olsen
S	Compilation of six Member Plaintiff account statements reflecting charge-offs prior to March 2019
T	Capital One account statements for Member Plaintiff Harold Velez, CAPITALONE_MDL_002205113
U	July 2015 web archive of CapitalOne.com Terms and Conditions
V	Declaration of Tami Kottke
W	Declaration of Kevin Kupiec
X	Representative Plaintiff Emily Behar Deposition Excerpts
Y	Representative Plaintiff Brandi Edmondson Deposition Excerpts
Z	Representative Plaintiff Emily Gershen Deposition Excerpts
AA	Representative Plaintiff Brandon Hausauer Deposition Excerpts

EXHIBIT LETTER	DESCRIPTION
BB	Representative Plaintiff Sara Sharp Deposition Excerpts
CC	Representative Plaintiff John Spacek Deposition Excerpts
DD	Representative Plaintiff Caralyn Tada Deposition Excerpts
EE	Representative Plaintiff Gary Zielicke Deposition Excerpts
FF	Member Plaintiff Amjed Ababseh Deposition Excerpts
GG	Member Plaintiff Michelle Baisden Deposition Excerpts
HH	Member Plaintiff Leticia Carter Deposition Excerpts
II	Member Plaintiff Isabel DeLeon Deposition Excerpts
JJ	Member Plaintiff Harold Velez Deposition Excerpts
KK	Plaintiffs' Expert Kevin Mitnick Deposition Excerpts
LL	Plaintiffs' Expert Gary Olsen Deposition Excerpts
MM	Capital One Application History Report for Brandon Hausauer, CAPITALONE_MDL_002021106
NN	Capital One Application History Report for Caralyn Tada, CAPITALONE_MDL_002018788
OO	Capital One Application History Report for Emily Gershen, CAPITALONE_MDL_002019493

INTRODUCTION

When Plaintiffs filed their operative complaint over a year ago, they alleged numerous injuries resulting from the actual misuse of their personal information, including identity theft and fraud. But discovery belied those allegations: Plaintiffs have *no* evidence that the hacker who perpetrated the data breach announced on July 29, 2019 ("Cyber Incident") ever misused or disseminated the data she stole. To the contrary, the evidence shows that promptly upon realizing it had been the victim of a cyberattack, Capital One worked with authorities to aid in the hacker's arrest, the seizure of her devices, and the recovery of the stolen data before it was ever misused.

Although Plaintiffs have no evidence that anyone suffered harm because of the Cyber Incident, they ask this Court to certify a 98-million-person nationwide class and award astronomical damages. But even if Plaintiffs' claims had merit (they do not), this case is fraught with individualized issues and is decidedly inappropriate for class treatment. While Plaintiffs seek uniform classwide damages tied to a purported increased "risk" of identity theft and damages for the lost "value" of their information, the record shows that *724* unique combinations of data elements were stolen in the Cyber Incident (the vast majority of which could *not* be used to commit fraud); that *all* Plaintiffs' information has been impacted in prior data breaches; and that half of the Plaintiffs experienced identity theft *before* the Cyber Incident ever occurred. The same issues exist when looking beyond the Representative Plaintiffs to the other plaintiffs named in member complaints consolidated in this MDL: of the 99 who answered discovery, nearly half were impacted in prior breaches, and nearly 20 percent were victims of identity theft before the Cyber Incident. Extrapolating these figures to the putative class more broadly, it is clear that millions of mini-trials would be required to determine whether *any* harms the putative class members claim to have suffered can be traced to the Cyber Incident. Because Plaintiffs' claims and alleged injuries

cannot be tried with common proof, a faithful and rigorous application of the Rule 23 factors demands that class certification be denied.

First, issues of Article III standing preclude class certification on Plaintiffs' negligence and statutory claims. The only injuries that can potentially support standing for those claims are actual identity fraud—and an imminent risk of identity fraud—traceable to the Cyber Incident. Here, however, Plaintiffs lack standing to press their tort and statutory claims, rendering the issue of class certification moot. Predominance is likewise absent because the law requires *all* putative class members to have Article III standing, and determining if individual class members have standing would require highly idiosyncratic inquiries concerning, *e.g.*, whether the individual suffered identity fraud, the causes and alleged injuries of any fraud, and whether the Cyber Incident placed that individual at an imminent risk of future fraud.

Second, Plaintiffs are neither typical nor adequate class representatives. Although the putative class includes nearly 34 million individuals who applied for but never received a Capital One credit card ("Applicants"), Plaintiffs are *all* Capital One cardholders ("Cardholders"), creating an irreconcilable divide. As Cardholders who entered into express contractual relationships with Capital One, for example, Plaintiffs *cannot* assert unjust enrichment claims—or seek disgorgement damages—on behalf of Applicants.

Third, Plaintiffs cannot satisfy Rule 23(b)(3)'s predominance requirement. The claims they seek to certify all require proof of causation *and* injury, and adjudicating those elements would necessitate untold individualized inquiries across the 98 million putative class members. The individual issues associated with each of Plaintiffs' theories of injury break down as follows:

- **"Increased Risk" Theory**: Based on the unfounded assumption that the putative class faces an increased risk of identity fraud due to the Cyber Incident, Plaintiffs seek damages for the cost of purchasing a "Cadillac" credit monitoring product. But Plaintiffs fail to show with common proof that putative class members face an *increased* risk *because of* the Cyber

Incident. Determining whether the Cyber Incident increased any individual's risk level would require highly individualized findings to, *e.g.*, (i) assess what information about that individual was already available to bad actors and (ii) compare that to the individual's information stolen in the Cyber Incident. This problem is not hypothetical: all the Plaintiffs have been impacted in prior breaches, half were victims of identity fraud *before* the Cyber Incident, and only two had sensitive data elements stolen in the Cyber Incident. The risk of fraud, if any, to any putative class member is unique.

- **"Market Value" Theory**: Plaintiffs seek damages for the "value of the hacker's unauthorized access" to putative class members' information. But Plaintiffs ignore that the "market value" of an individual's information (if there is such a thing) varies considerably depending on what specific data elements about that individual were exposed and characteristics specific to the individual. As the Court previously held, this theory also fails without evidence that an individual would be willing to sell her information in the first place—yet another individualized question and one to which each Plaintiff answered "no."

- **"Disgorgement" Theory**: Plaintiffs seek disgorgement in the amount of fraud Capital One prevented between 2015 and 2020 using its proprietary fraud models (some of which used stolen credit card application data as one input among many). But Plaintiffs' disgorgement theory—which baselessly assumes that each class member's application data conferred the same "unjust" benefit on Capital One—raises myriad individualized issues. Capital One's fraud models did not even use most putative class members' application data during the relevant time period. And determining whether a fraud model actually used any individual's data—and if so, whether and what amount of fraud was thereby prevented—would be a hopelessly individualized task. Worse still, Plaintiffs gloss over the real, but individualized, benefits putative class members received from Capital One's enhanced fraud defenses.

Predominance is also destroyed by an abundance of individualized questions specific to Plaintiffs' common-law and statutory claims. These questions arise from, among other things, (i) dramatic variation in the materials and disclosures underlying the putative class members' contract claims over the 15-year class period; (ii) issues of causation specific to each putative class member's claimed injuries; and (iii) a variety of defenses that Capital One would assert based on each putative class member's own particular circumstances, including the defenses of statute of limitations, first material breach/setoff, failure to mitigate/contributory negligence, and release.

Fourth, because of the numerous obstacles to class certification on their primary injury theories, Plaintiffs ask the Court to certify a nationwide breach-of-contract class seeking nominal damages. The Court should reject this invitation. Contrary to Plaintiffs' contention, a request for

nominal damages does not relieve Plaintiffs and the putative class members from the need to *individually* prove that they were each *injured* by Capital One's alleged breach of contract. And certifying a nominal-damages-only class would be far from "superior" to other methods for adjudicating Plaintiffs' claims.

Finally, Plaintiffs are not entitled to an "injunctive-relief" class because no putative class member faces an "imminent risk" of suffering harm from another, similar breach at Capital One. The issues that led to the Cyber Incident have all been remediated, and Capital One has also made comprehensive improvements to its overall cybersecurity defenses. Nor is issue certification proper—certifying the issues of duty and breach, as Plaintiffs propose, would do virtually nothing to move this litigation closer to a final disposition.

RELEVANT FACTS

I. CONSUMERS APPLY FOR CAPITAL ONE CREDIT CARDS IN VARIOUS WAYS

Because the personal data stolen in the Cyber Incident consists of information consumers submitted to Capital One when applying for credit cards, the application channels they used and the varied circumstances surrounding their applications are relevant. The approximately 98 million putative class members applied for different types of credit cards from 2005 to 2019. They applied in different ways, for different reasons, and at different times.

This considerable variation is illustrated by considering just a handful of individuals—the Representative Plaintiffs ("Plaintiffs") and the member plaintiffs named in complaints consolidated into this MDL ("Member Plaintiffs").[1] [redacted]

[redacted]

[1] Because there are millions of putative class members, the differences discussed here are undoubtedly more pronounced in the broader putative class.

[redacted]. *See, e.g.*, Member Pl. Ababseh Dep. 45:12–46:21. [redacted]. *See* Sharp Dep. 52:16–54:1, 69:18–70:8; Zielicke Dep. 36:17–37:20.

Their reasons for applying also varied. Some applied for partnership credit cards to access the rewards program. *See id.* [redacted], Gershen Dep. 32:15–33:3, [redacted], Member Pl. Carter Dep. 23:6-25. Further, [redacted]. *See* Member Pl. Baisden Dep. 55:13–56:12; Zielicke Dep. 36:5–38:14. Similarly, [redacted]. *See* Ex. A (Edmondson HSBC card statements); Declaration of Tami Kottke ¶ 3 (HSBC acquired by Capital One in 2012).

Additionally, Plaintiffs, Member Plaintiffs, and putative class members received widely disparate disclosures in the application process. Kottke Decl. ¶¶ 10-12. Contrary to Plaintiffs' assertion, "each [A]pplicant" did *not* receive Capital One's Privacy and Opt-Out Notice ("Privacy Notice") (on which Plaintiffs' breach-of-contract claim is based) in the application process. Dkt. 1260, Pls.' Motion ("Mot.") at 2. [redacted]. Behar Dep. 38:10–39:2; Member Pl. Ababseh Dep. 45:12–46:21. Phone applicants received no written materials, Kottke Decl. ¶¶ 21, 32, and whether individuals who applied in response to mail solicitations were provided access to the Privacy Notice depends on the date the solicitation was sent and the application method that person chose. *Id.* ¶¶ 16, 18, 20-21; Ex. C; Tada Dep. Exs. 5055, 5057. Other applicants, such as Plaintiffs Gershen, Hausauer, Spacek, and Tada, [redacted]

[redacted]. Kottke Decl. ¶ 18; Gershen Dep. 66:18-23; Hausauer Dep. 41:25–42:5, 88:2-16; Spacek Dep. 72:8-19, 74:24–75:5; Tada Dep. 51:13–52:2, 63:22–64:3. In some cases, online applications included a link to the Privacy Notice, along with an acknowledgement that the applicant read and agreed to the Privacy Notice. Kottke Decl. ¶ 18; Ex. D. Other putative class members applied at a Capital One branch, café, or kiosk, or through a Capital One mobile application, where a link to Capital One's Privacy Notice may (or may not) have been available depending on the time of the application. Kottke Decl. ¶¶ 19, 22-23.

With respect to consumers who applied for partnership cards, the application process differed depending on the partner and channel. *Id.* ¶¶ 24-32. [redacted] Zielicke Dep. 36:17–37:16, 42:18–44:20, 45:4-17, 47:20–48:3, 49:17–52:3, 66:18–70:10; Zielicke Dep. Ex. 5002. [redacted]. Sharp Dep. 52:12–55:24. Overall, each retail partner works with Capital One to determine the contours of the application process for each application channel and to decide what information will be provided at the time of application. Kottke Decl. ¶ 24. Some, but not all, of Capital One's partners included a link to the Privacy Notice in their online applications. *Id.* ¶¶ 29-31. None of Capital One's partners provided a copy of the Privacy Notice with paper applications. *Id.* ¶ 26.

Moreover, the content of the documents provided to Applicants and Cardholders has varied over time. Capital One's Privacy Notice, which explains how the company uses customer information and how customers can limit Capital One's sharing of their information, underwent

significant changes in 2010. *Compare* Mot. Ex. 31, Dkt. 1260-32 (2009 Privacy Notice) *with* Mot. Ex. 32, Dkt. 1260-33 (2018 Privacy Notice). Specifically, in 2010, Capital One added the language Plaintiffs primarily rely on for their breach of contract claim, which states that Capital One uses security measures that "comply with federal law" to "protect" personal information from "unauthorized access and use." Dkt. 1260-33 at 3; Mot. at 2-3; Dkt. 971 ¶¶ 96, 215. Before 2010, the Privacy Notice did not contain that language. *See* Dkt. 1260-32.

II. THE CYBER INCIDENT AND THE STOLEN DATA

A. Overview of the Cyber Incident and Capital One's Response

On July 29, 2019, Capital One announced that it had been targeted in a criminal cyber-attack in which a hacker, Paige Thompson, stole personal information of approximately 98 million of its U.S. credit card customers and applicants. *See* Ex. E at 3-5. Thompson was arrested that day, and her electronic devices were seized. Critically, there is no evidence that the stolen information has been disseminated or misused. *See* U.S. Opp. to Mot. for Revocation of Detention Or. at 6, *United States v. Thompson*, 2:19-mj-00344-MAT (W.D. Wash. Sept. 20, 2019), ECF No. 49; Ex. F. Before the announcement, Capital One had promptly alerted law enforcement to its discovery of the Cyber Incident [redacted]. Dkt. 1348-2, Capital One's Third Supp. Resp. to Interrog. No. 12 at 2, 11.

Immediately following discovery of the Cyber Incident, Capital One fixed the issue that allowed the breach to occur and began implementing security improvements to prevent future breaches. *Id.* at 2, 11-13. Capital One has since engaged in longer-term efforts to strengthen its overall cybersecurity defenses. *Id.* at 3-10, 13-46. [redacted]. *See* Ex. G at 59-66.

B. The Widely-Varying Data Impacted in the Cyber Incident

The data Paige Thompson accessed was generally non-sensitive. Only 0.2% of the putative class members had their Social Security Numbers ("SSNs") or bank account numbers taken. For the other 99.8% of the putative class, the stolen data consists largely of [redacted]. *See* Ex. E at 7-8. Thompson [redacted] *Id.* at 7. [redacted]. Ex. H ¶ 100. For example, [redacted] *See* Mot. Ex. 25, Dkt. 1260-26. By contrast, neither [redacted] *Id.* None of that data could be used to identify [redacted]. Notably, each Plaintiff's information [redacted]. *See* App'x A.

[2] [redacted] *See* Ex. I at 19; Mot. at 12 n.12. Based on accepted definitions of the term "PII" or "Personally Identifiable Information," [redacted] Mot. at 15.

Most of the stolen data could not be used to commit fraud, identity theft, or other financial crimes. [redacted] Ex. I at 10. In fact, basic information such as a person's name, date of birth, and address are often publicly available. *Id.* at 13. Proving that point, Capital One's expert Rebecca Kuehn confirmed [redacted]. *Id.* at 13-14. Notably, [redacted] *See* App'x A.

Other commonly impacted data elements, such as self-reported income, credit scores, and transaction information, cannot be used to commit fraud or identity theft, either. *Id.* at 12. Thus, the stolen data for each putative class member, as well as the prior availability of his information, must be examined to determine if any risk of fraud is attributable to the Cyber Incident.

III. PROCEDURAL HISTORY

A. Plaintiffs and Their Claims

Plaintiffs are eight Capital One Cardholders from six states whose information was stolen in the Cyber Incident. *See* Dkt. 1130 at 2; Dkt. 971 ¶¶ 18-25. On September 18, 2020, the Court granted in part Defendants' motions to dismiss. *See* Dkt. 879. On May 7, 2021, the Court ruled that Virginia law governs Plaintiffs' common-law claims. *See* Dkt. 1293. After these orders, the following claims remain pending against Capital One: negligence, breach of express contract, breach of implied contract, breach of confidence,[3] unjust enrichment, declaratory judgment, and

[3] The Court initially allowed Plaintiffs' breach of confidence claim to proceed under California law only, *see* Dkt. 879 at 40, but that claim is now extinguished given the Court's ruling that Virginia law applies to Plaintiffs' common-law claims. *See* Dkt. 1293.

certain state statutory claims. Plaintiffs do not seek to certify a class with respect to all of these claims, nor do they seek relief under Rule 23 for many of the injuries they allege they suffered.

B. Plaintiffs' Motion for Class Certification

Plaintiffs seek certification of a nationwide class of individuals whose data was stolen in the Cyber Incident and a variety of alternative and state subclasses. Mot. at 15-17. Plaintiffs also seek certification of an injunctive-relief class under Rule 23(b)(2). *Id*. at 37-39. In the alternative, Plaintiffs request certification of "issues-based classes" under Rule 23(c)(4). *Id*. at 40. The table below summarizes the claims and alleged harms for which Plaintiffs seek certification, along with the corresponding classes to which those theories of recovery relate and the Representative Plaintiff(s) proposed to represent each class:

CLAIM	ALLEGED HARM(S)	PROPOSED CLASS(ES)	REPRESENTATIVE PLAINTIFF(S)
Breach of Contract (or, in the alternative, breach of implied contract)	• Nominal Damages • Market Value • Increased Risk • Disgorgement	Applicant Class	All Representative Plaintiffs
		Cardholder Subclass	All Representative Plaintiffs
		SSN / Bank Account Subclass	Behar and Hausauer
Negligence	• Market Value • Increased Risk	Applicant Class	All Representative Plaintiffs
		Cardholder Subclass	All Representative Plaintiffs
		SSN / Bank Account Subclass	Behar and Hausauer
Unjust Enrichment	• Market Value • Disgorgement	Applicant Class	All Representative Plaintiffs
		Cardholder Subclass	All Representative Plaintiffs
		SSN / Bank Account Subclass	Behar and Hausauer
Declaratory Judgment	• Continuing Risk of Harm from Capital One's Retention of PII	Applicant Class	All Representative Plaintiffs
		Cardholder Subclass	All Representative Plaintiffs

CLAIM	ALLEGED HARM(S)	PROPOSED CLASS(ES)	REPRESENTATIVE PLAINTIFF(S)
		SSN / Bank Account Subclass	Behar and Hausauer
		California Subclass	Hausauer and Tada
		California CLRA Subclass	Tada
		Washington Subclass	Sharp
California Unfair Competition Law ("UCL")	• None identified	California Subclass	Hausauer and Tada
California Consumers Legal Remedies Act ("CLRA")	• None identified	California CLRA Subclass	Tada
New York General Business Law ("GBL")	• None identified	New York Subclass	Gershen
Washington Consumer Protection Act ("WCPA")	• None identified	Washington Subclass	Sharp

Plaintiffs do not seek certification of any claims arising from *actual* identity theft or fraud, despite alleging in their original Complaint that they would be forced to "contend with the loss of th[eir] valuable data and resultant and imminent identity theft and fraud." Dkt. 332 ¶ 5. In fact, Plaintiffs have abandoned any prospect of classwide recovery for a broad swath of the harms alleged in the Complaint, including: "identity theft and fraud"; "unauthorized charges and loss of use of and access to their financial account funds"; "lowered credit scores resulting from credit inquiries following fraudulent activities"; and "costs associated with time spent . . . to mitigate and address the actual and future consequences of the Data Breach." Dkt. 971 ¶ 140.

RULE 23 LEGAL STANDARD

"The class-action device . . . is an exception to the general rule that a party in federal court may vindicate only his own interests." *Thorn v. Jefferson-Pilot Life Ins. Co.*, 445 F.3d 311, 318 (4th Cir. 2006). This Court "must conduct a 'rigorous analysis'" of Plaintiffs' motion, "paying 'careful attention to the requirements of'" Rule 23. *Id*. at 318. Plaintiffs must "affirmatively demonstrate" their "compliance" with every requirement of Rule 23(a) and at least one of the three requirements in Rule 23(b). *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 345 (2011). "[T]he plaintiffs bear the burden in this regard . . . and the district court is required to make findings on whether the plaintiffs carried their burden." *Gariety v. Grant Thornton, LLP*, 368 F.3d 356, 370 (4th Cir. 2004). Plaintiffs also bear the burden of "establishing that damages are capable of measurement on a classwide basis." *Comcast Corp. v. Behrend*, 569 U.S. 27, 34 (2013).

Additionally, because Plaintiffs' request for certification hinges on expert opinions, the Court must rigorously analyze those opinions. In the Fourth Circuit, "only reliable evidence must be considered in deciding class certification because reliability of evidence is a fundamental dictate of *Daubert*." *Soutter v. Equifax Info. Servs. LLC*, 299 F.R.D. 126, 131 (E.D. Va. 2014); *Childress v. JPMorgan Chase & Co.*, 2019 WL 2865848, at *2 (E.D.N.C. July 2, 2019) ("[W]here a movant has proffered expert testimony in support of its motion for class certification, and such testimony is critical to the issue of class certification, a full *Daubert* inquiry is appropriate.").

ARGUMENT

I. PLAINTIFFS CANNOT PROVE STANDING, NOR COULD STANDING BE PROVEN FOR THE PUTATIVE CLASS THROUGH COMMON PROOF.

As a threshold matter, issues of Article III standing preclude certification of Plaintiffs' negligence and state statutory claims.

First, as explained in Capital One's Motion Suggesting Lack of Jurisdiction, Plaintiffs lack Article III standing to assert their negligence and state statutory claims. *See* Dkt. 1386. The Court should therefore dismiss those claims for lack of jurisdiction, rendering the request for class certification moot. *See O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) ("[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.").[4]

Second, even if the Court holds that Plaintiffs have standing, it cannot certify a class containing absent class members who do not. Therefore, Plaintiffs must define the proposed classes to include only putative class members with Article III standing to assert each claim. *See Denney v. Deutsche Bank AG*, 443 F.3d 253, 264 (2d Cir. 2006) ("[N]o class may be certified that contains members lacking Article III standing."); *Branch v. Gov't Emps. Ins. Co.*, 323 F.R.D. 539, 552 (E.D. Va. 2018) (same). Plaintiffs have ignored this bedrock jurisdictional requirement, and instead ask the Court to certify a nationwide class (and various state subclasses) of all individuals whose data was stolen in the Cyber Incident—irrespective of whether they suffered any injury-in-fact traceable to the Cyber Incident. *See* Mot. at 15-17. The only injuries Plaintiffs assert in their Motion to support standing for their negligence and state statutory claims are actual identity theft and an imminent risk of identity theft. *Id.* at 17-19. Yet, determining whether any putative class members suffered such an injury would require conducting millions of mini-trials on issues concerning (among other things): (i) whether any instances of fraud were traceable to the Cyber

[4] Plaintiffs base their "standing" on the fact that the Court previously found their *allegations* of identity fraud sufficient at the motion to dismiss stage. Mot. at 18-19. But Rule 23 imposes evidentiary requirements; allegations are insufficient. *See*, *e.g.*, *Ang v. Bimbo Bakeries USA, Inc.*, 2018 WL 4181896, at *4 (N.D. Cal. Aug. 31, 2018) ("Rule 23's requirement that plaintiffs prove their entitlement to class certification by a preponderance of the evidence . . . require[s] Plaintiffs to make some evidentiary showing that they have standing, rather than simply alleging as much.").

Incident, (ii) what specific data elements were exposed for an individual, and (iii) whether such data was previously exposed in a prior data breach or publicly available through other means.

These questions cannot be answered using common evidence. Accordingly, the Court cannot certify any of the proposed classes as to Plaintiffs' negligence and state statutory claims. *See Branch*, 323 F.R.D. at 552 ("prevalence of particularized factual issues" regarding which class members have standing "prevent [plaintiff] from satisfying the predominance requirement").[5]

II. PLAINTIFFS ARE NEITHER TYPICAL NOR ADEQUATE REPRESENTATIVES.

Under Rule 23(a)(3), "the claims or defenses of the representative parties [must be] typical of the claims or defenses of the class." Fed. R. Civ. P. 23(a)(3). That is, a representative "plaintiff's claim cannot be so different from the claims of absent class members that their claims will not be advanced by plaintiff's proof of his own individual claim." *Deiter v. Microsoft Corp.*, 436 F.3d 461, 466-67 (4th Cir. 2006). To evaluate typicality, the Court must compare "the plaintiffs' claims or defenses with those of the absent class members" to ensure they are sufficiently similar. *Id.* Further, Rule 23(a)(4) requires Plaintiffs to demonstrate that they "will fairly and adequately protect the interests of the class," Fed. R. Civ. P. 23(a)(4), meaning there can be no "conflicts of interest between named parties and the class they seek to represent." *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 625 (1997). The Plaintiffs in this case fail both tests.

Although the alleged class includes 33.8 million Applicants, *no* Plaintiff is an Applicant. Rather, "each Plaintiff named in the Representative Complaint" is a "Capital One cardholder" with a "Cardholder Agreement." *See* Dkt. 1130 at 2. This critical difference drives a wedge between

[5] Relatedly, even if the Court held that certain Plaintiffs had suffered an Article III injury (such as identity theft) traceable to the Cyber Incident, Plaintiffs would be atypical of putative class members who suffered no such injury. *See Wal-Mart*, 564 U.S. at 345 (typicality demands that named plaintiffs "suffer the same injury as the class members"); *see also TransUnion LLC v. Ramirez*, 141 S. Ct. 972 (2020) (granting *certiorari* on related issues of standing and typicality).

Plaintiffs and the Applicants they seek to represent, revealing fatal shortcomings as to both typicality and adequacy.

A. Plaintiffs Cannot Assert Contractual or Quasi-Contractual Claims on Behalf of Absent Class Members, Destroying Typicality.

The typicality requirement demands, at a minimum, that "a class representative must be part of the class and possess the same interest and suffer the same injury as the class members." *Deiter*, 436 F.3d at 466 (quotation omitted). Here, Plaintiffs are not typical of the putative class members in at least two critical respects.

First, as will be shown in Capital One's forthcoming Motion for Summary Judgment, Plaintiffs cannot bring claims for unjust enrichment or breach of implied contract because they have express contracts with Capital One covering the subject matter of those claims. *See* Capital One's Mot. for Summ. J. ("MSJ"). Therefore, they cannot represent the nearly 34 million absent Applicant class members—who lack contracts with Capital One—for purposes of their unjust-enrichment and implied-contract claims. *See Weinberger v. Retail Credit Co.*, 498 F.2d 552, 556 (4th Cir. 1974) (named plaintiff not typical where his claim was time-barred, excluding him from "the class he seeks to represent").

Second, Plaintiffs' and Applicants' breach of contract claims are significantly different. Plaintiffs argue that "the Privacy Notice contains enforceable contractual promises with respect to the entire class, including [Applicants]." Mot. at 3 n.4. But while Capital One admits that the Privacy Notice is incorporated into Plaintiffs' Cardholder Agreements, it vigorously contests that the Privacy Notice constitutes a standalone contract with Applicants. As explained below, because Applicants never entered into a Cardholder Agreement with Capital One, they must show "mutuality of assent" and present individual proof concerning the components of any purported agreement they struck with Capital One. *See Phillips v. Mazyck,* 643 S.E.2d 172, 175 (Va. 2007).

This analysis will require evaluating the circumstances under which each Applicant applied and which statements concerning data security (if any) he or she viewed or relied on. Consequently, the Plaintiffs' and Applicants' breach of contract claims do not depend on "the same factual and legal arguments," raising the "possibility that there was a breach of contract with some class members, but not with other[s]." *Broussard v. Meineke Discount Muffler Shops, Inc.*, 155 F.3d 331, 340 (4th Cir. 1998).[6]

B. The Dichotomy Between Plaintiffs and Putative Applicant Class Members Also Defeats Adequacy.

It is "axiomatic that a putative representative cannot adequately protect the class if the representative's interests are antagonistic to or in conflict with the objectives of those being represented." *Plotnick v. Comput. Scis. Corp. Deferred Comp. Plan*, 182 F. Supp. 3d 573, 584 (E.D. Va. 2016), *aff'd*, 875 F.3d 160 (4th Cir. 2017). Here, the fact that none of the Plaintiffs are Applicants makes them inadequate to represent putative Applicant class members.

Plaintiffs have failed to adduce evidence that would support Applicants' contract claims, underscoring their inadequacy to represent Applicants. Plaintiffs assert that as "part of [the application] process, "each applicant is provided with Capital One's Privacy Notice." Mot. at 2. But they cite no evidence—and there is none. Under the Gramm-Leach-Bliley Act ("GLBA"), Capital One is only required to provide a Privacy Notice "when [it] establish[es] a customer relationship" with a consumer. *See* 12 C.F.R. § 1016.4(a); s*ee also id.* § 1016.4(c) ("customer relationship" established by entering into "a continuing relationship," such as "[o]pening a credit

[6] The Cardholder-Applicant divide also renders Plaintiffs' negligence claim atypical of Applicants' negligence claim. Under Virginia's economic loss doctrine, a plaintiff may not recover in tort for the breach of a duty assumed by contract. *See Tingler v. Graystone Homes, Inc.*, 834 S.E.2d 244, 261 (Va. 2019). The economic loss doctrine therefore precludes Cardholders—who claim that their contracts with Capital One contain obligations regarding data security—from recovering in negligence, whereas that defense would not apply to Applicants.

card account"). Plaintiffs have not developed evidence—and certainly not common evidence—demonstrating that Applicants were presented with the Privacy Notice, read or relied on the Privacy Notice, or otherwise formed a contract with Capital One based on the Privacy Notice at the time of their applications. Plaintiffs' failure to do so shows they cannot "fairly and adequately protect the interests" of absent Applicant class members.

This failing is emblematic of a broader class conflict stemming from the Applicant-Cardholder divide: while Plaintiffs, as Cardholders, are incentivized to pursue their breach-of-express-contract claim, Applicants (who would not benefit from that claim) are incentivized to pursue quasi-contractual claims, such as unjust enrichment. Plaintiffs do not share those incentives because they *do not have and cannot pursue* an unjust enrichment claim, as they have conceded. *See* Dkt. 1129, Jan. 12, 2021 Hr'g Tr. at 23-24. Thus, because Plaintiffs and Applicants "have potentially divergent aims" that produce a "conflict in remedial interests," adequacy is not satisfied. *See Broussard*, 155 F.3d at 338-39.

III. PLAINTIFFS CANNOT ESTABLISH PREDOMINANCE FOR ANY CLAIM.

A. Individualized Inquiries Would be Required to Establish Causation and Injury for Each Class Member.

To certify a damages class under Rule 23(b)(3), Plaintiffs must prove that "questions of law or fact common to class members predominate over any questions affecting only individual members." Fed. R. Civ. P. 23(b)(3). The predominance inquiry is "demanding," *Amchem*, 521 U.S. at 624, and serves to "test[] whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Lienhart v. Dryvit Sys., Inc.*, 255 F.3d 138, 147 (4th Cir. 2001). Where the "elements [of a claim] can only be established after considerable individual inquiry," common questions do not predominate. *Sustainable Forest L.L.C v. Qwest Comms. Int'l, Inc.*, 2005 WL 8146267 (D.S.C. 2005) (citation omitted). Predominance is not met here because the

elements of causation and injury, which Plaintiffs must establish for *all* of their claims, depend upon highly individualized proof. That is true for all of Plaintiffs' theories of harm: (1) the "Increased Risk" theory; (2) the lost "Market Value" theory; and (3) the "disgorgement" theory.

Even if Plaintiffs could establish the elements of injury and causation with common proof, they independently fail the predominance test because their damages models fail to "measure only those damages" attributable to their theories of injury, as required by *Comcast*. 569 U.S. at 35. As shown below, properly measuring damages in this case would require individualized inquiries, and predominance is not shown where "[q]uestions of individual damage calculations . . . inevitably overwhelm questions common to the class." *Id.* at 34.

1. Plaintiffs Cannot Prove their "Increased Risk" Theory on a Classwide Basis.

Plaintiffs' expert Kevin Mitnick offers opinions about how malicious actors *could* theoretically misuse the stolen data. *See generally* Mot. Ex. 15, Dkt. 1260-16, Am. Expert Rep. of Kevin Mitnick. He concludes that, because of this theoretical risk, *all* class members should be awarded the cost of five years' worth of premium credit monitoring services. *See* Mot. at 10-11, 13 (arguing the "stolen PII can be used to commit identity theft" and therefore "each member of the class" needs credit monitoring to prevent future harm). Plaintiffs assert the Increased Risk theory of injury as to their breach of contract and negligence claims. *See id.* at 30, 34.

Mitnick's starting point is the (erroneous) assumption [redacted]. *See* Mitnick Dep. at 68:16-69:14. Based on that false assumption, [redacted] Dkt. 1260-16 ¶¶ 24-25, 27. Mitnick posits [redacted]. *Id.* ¶¶ 25, 34. [redacted], Mitnick Dep.

58:15-19, 68:12-14—Mitnick concludes that [redacted]. Dkt. 1260-16 ¶ 63. Accordingly, he opines [redacted]. *Id.* ¶¶ 70-71.

In turn, Plaintiffs' expert Terry Long takes [redacted] Mot. Ex. 26, Dkt. 1260-17, Expert Rep. of Terry Long at 1-2. [redacted] *Id.*

a. Plaintiffs' Increased Risk Theory Should be Rejected.

Initially, putative class members face no risk of harm, much less an increased risk, because there is no evidence that the Capital One data was ever misused or disseminated by Thompson. *See* MSJ. [redacted]. Mitnick Dep. 55:1–56:17. Plaintiffs thus have not suffered an increased risk of harm and are not entitled to damages on this theory. *See* Dkt. 1386; *see also* MSJ. Regardless, Plaintiffs cannot prove their Increased Risk injury with common proof.[7]

b. Plaintiffs' Increased Risk Theory Does Not Satisfy the Predominance Requirement of Rule 23.

Fundamentally, the level of risk any putative class member faces depends on his or her individual circumstances. Mitnick, [redacted]

[7] Moreover, as explained in Capital One's motions to exclude Mitnick and Long, Dkt. Nos. 1390, 1395, the expert opinions on which Plaintiffs' Increased Risk theory is based are fundamentally flawed, irrelevant, and unreliable and should be excluded under Federal Rule of Evidence 702.

[redacted]. *See* Mitnick Dep. 185:3–186:12, 188:14–191:6. This variation in risk levels stems from several different individual factors.

Prior Exposure. The extent to which the Capital One Cyber Incident *increased* any putative class member's risk of future harm (over and above any existing risk) necessarily depends on whether that individual's data was already accessible to bad actors before the Cyber Incident (and if so, the type and amount of data that was accessible). *See Gardner v. Health Net, Inc.*, 2010 WL 11579028, at *4-5 (C.D. Cal. Sept. 13, 2010) (denying certification due to the need for individualized inquiries regarding "whether each class member actually suffered [harm] . . . traceable to the stolen [data]" and noting such harm could have "any number of causes" because breaches happen "frequently").

Discovery has revealed that [redacted]. *See* App'x A. [redacted]. *See id.* [redacted]. *Id.* [redacted]. *Id.* Plaintiffs' data was also exposed publicly in other ways.[8] Capital One's expert Kuehn [redacted] *See* Ex. I at 13-14.

[8] For example, [redacted]. *See* Ex. J at 3; Ex. K. [redacted]. *See* Ex. L at 3; Ex. M at 3; Ex. N at 3; Ex. O at 3; Spacek Dep. 190:2–191:7.

The same is true with respect to Member Plaintiffs. [redacted], *see* Ex. B, [redacted], *see* Ex. P. There is no doubt that millions of putative class members' data has also been exposed or misused due to prior breaches, or is otherwise publicly available. Data breaches have become so common that the director of the U.S. Financial Crimes Enforcement Network recently concluded that "there is a high likelihood that most users of the U.S. financial system have had some information about themselves … compromised." Ex. I at 17. [redacted] Mitnick Dep. 222:7-224:14; *see also id.* (testifying [redacted].

Mitnick also admits [redacted]. *See* Ex. Q, Expert Rebuttal Rep. of Kevin Mitnick ¶ 28 [redacted] Thus, understanding whether, or to what extent, any individual's risk level *increased* as a result of the Cyber Incident requires case-by-case examination—including analysis of (i) the number of prior breaches/exposures, (ii) the type of information exposed, and (iii) the overlap between previously exposed data and the data at issue here. [redacted]

[9] The Court permitted Capital One to serve discovery on Member Plaintiffs in the form of "fact sheets," which required information about the factual support for each Member Plaintiff's claims (*e.g.*, how they contend they were harmed by the Cyber Incident). Rather than responding, the vast majority of Member Plaintiffs voluntarily dismissed their claims. Dkt. 834 at 12.

[redacted]. Dkt. 1260-16 ¶¶ 24, 25 & Ex. C. [redacted], Ex. I at 13-14, [redacted]. In fact, [redacted], *see* Mitnick Dep. 63:4-23, 64:20-24, [redacted]. Dkt. 1260-16 ¶¶ 24-25.

Proving a causal link between the Cyber Incident and Plaintiffs' Increased Risk injury is thus an inherently individualized issue that defeats predominance. *See Lienhart*, 255 F.3d at 147 ("[T]he need for individualized proof of damages may defeat predominance where proof of damages is essential to liability.")

Plaintiffs' suggestion that the "concurrent cause doctrine" relieves them of the need to prove causation is wrong. *See* Mot. at 33. In Virginia, this tort doctrine applies only "where two causes concur to bring about an event and *either alone* would have been *sufficient* to bring about an identical result." *Ford Motor Co. v. Boomer*, 736 S.E.2d 724, 731 (Va. 2013) (emphasis added). In other words, the "concurrent cause doctrine" applies only where any of several different causes would itself be sufficient to produce the harm complained of. Here, Plaintiffs cannot prove causation without evidence of dissemination, and even if they could, individualized inquiries of each putative class member would be required to determine whether the Cyber Incident itself *increased* any class member's risk of fraud above their baseline level of risk.

Variation in Impacted Data Elements. Putative class members had a wide variety of data elements impacted by the Cyber Incident. [redacted] Ex. H ¶ 100, [redacted]

Ex. I at 10 [redacted] Mitnick concedes [redacted], Mitnick Dep. 185:20–186:1, [redacted]. *See* Mitnick Dep. 55:1–56:17; Ex. I at 19. But neither Mitnick nor Plaintiffs account for these individualized factors. Additionally, an individual's level of risk—and whether (and to what extent) it has increased due to the Cyber Incident—is affected by other factors specific to that person, such as differences in income, credit limits, and whether an individual's information has changed over time. *See* Dkt. 1390 at 25-26.

Presumably, [redacted]. *See* Dkt. 1260-16 ¶¶ 24-28, 70; Mot. at 10-11. But there is no evidence that such enrichment has taken place. Indeed, Mitnick's theory is not even about "enriching" stolen Capital One data—it is about constructing a new data set from *other* sources. And it depends on the assumptions that putative class members' data, including SSNs, are otherwise available and that a criminal could obtain the data through other sources. Such speculation violates *Comcast*, because it does not measure "only those damages attributable" to the Cyber Incident. *See* 569 U.S. at 35; *see also Town of W. Point v. Evans*, 299 S.E.2d 349, 351 (Va. 1983) (causation cannot be proved with "conjecture, guess, or random judgment").

Regardless, determining the extent to which any putative class member's data has been or is capable of being "enriched" in the manner Mitnick suggests would require individualized proof. For instance, what data is available from other sources about an individual class member? And would that data, in combination with the data exposed in the breach, allow a criminal to commit

fraud? Because putative class members can only establish a purported Increased Risk "injury through individual proof, the resulting inefficiency defeats predominance." *See In re Zetia (Ezetimibe) Antitrust Litig*, 2020 WL 5778756, at *16 (E.D. Va. Aug. 14, 2020).

Plaintiffs' Inappropriate Remedy. The varying levels of risk (if any) faced by putative class members necessarily means they require varying levels of mitigation (if any). This means that Plaintiffs' credit monitoring damages are incapable of classwide proof, *i.e.*, they must be calculated based on each putative class member's unique risk profile. *See Steering Comm. v. Exxon Mobil Corp*., 461 F.3d 598, 602 (5th Cir. 2006) (certification improper where open issues on damages included "location, exposure, dose, susceptibility to illness, nature of symptoms, type and cost of medical treatment, and subsequent impact of illnesses"). Moreover, whether any given putative class member requires credit monitoring (and if so, for how long) depends on additional individual factors such as other mitigation efforts (if any) he may have independently undertaken.

In sum, Plaintiffs' Increased Risk theory is incapable of classwide resolution. *See McGlenn v. Driveline Retail Merch., Inc*., 2021 WL 165121 at *9-10 (C.D. Ill. Jan. 19, 2021) (denying certification in data breach case due to individualized questions of damages and causation, including prior exposure); *Dolmage v. Combined Ins. Co. of Am.,* 2017 WL 1754772, at *7 (N.D. Ill. May 3, 2017) (denying certification where "Plaintiff's own damages expert makes clear that the types and amounts of damages suffered by class members will vary dramatically").

2. <u>Plaintiffs Cannot Prove Their "Market Value" Theory on a Classwide Basis.</u>

For their next theory of harm, Plaintiffs proffer the opinion of Gary Olsen, [redacted] *See* Mot. at 34; *see also* Mot. Ex. 6, Dkt. 1260-7, Am. Expert Rep. of Gary Olsen ¶ 52. Plaintiffs contend the Market Value theory of harm applies to their breach of contract, negligence, and unjust enrichment claims. *See* Mot. at 30, 32 n.23, 34.

Olsen purports to calculate the "damage" the putative class allegedly suffered when Thompson obtained "unauthorized access" to their information without compensating them. *See* Olsen Dep. 76:17–77:1. That is, he purports to measure "the value of a one-time nonexclusive access to the PII." *Id.* 40:22–41:2; *see also* Mot. at 13 ("[C]lass members lost the value of the unauthorized access to their PII."). To calculate the value of this "unauthorized access," Olsen relies [redacted]. Dkt. 1260-7 ¶¶ 5-6, 53, 55. [redacted]. *See id.* ¶¶ 5, 55. [redacted]. *See id.* ¶ 60.

As an initial matter, the Court has already rejected Plaintiffs' theory of harm premised on losing the inherent value of their PII. Dkt. 879 at 29. The "Market Value" injury Plaintiffs now advance is a deeply flawed riff on the same theory—it merely repackages that theory to focus on the inherent value of "access" to PII rather than a loss of the inherent value of the PII itself. In any event, Olsen's Market Value opinion is inadmissible under *Daubert* and the Federal Rules of Evidence, *see* Dkt. 1432, insufficient to confer Article III standing, *see* Dkt. 1386, and precluded by Virginia law, *see* MSJ. More importantly, it cannot satisfy the predominance requirement because individualized inquiries regarding injury and causation predominate over any common questions, and because it fails to satisfy the requirements of *Comcast* and *Wal-Mart*.

a. Individualized Inquiries Regarding Injury Predominate.

Under Plaintiffs' Market Value theory, determining whether an injury occurred at all—and if so, in what amount—would require case-by-case determinations, defeating predominance.

First, Olsen fails [redacted] The premise of Plaintiffs' Market Value theory is that the "use of PII should be

exclusively controlled by" consumers, and thus, Plaintiffs should be compensated for Thompson's "unauthorized" access. *See* Dkt. 1260-7 ¶ 53. But if a putative class member's data is already in the public domain, then it can be accessed by anyone—meaning the putative class member did not have "control" over the data and thus has not lost the value of "unauthorized access" to it. Notably, Olsen [redacted] Olsen Dep. 82:1-7.[10] To assess whether any putative class member suffered Plaintiffs' Market Value injury would require determining which data elements are already publicly available or offered for sale on the Dark Web. *See* Ex. H ¶ 74 (noting the value of stolen data depends on whether it is novel or already accessible). This must be done on an individual basis, as each individual's circumstances are unique. Because there is "no reliable means of proving classwide injury," common questions "cannot predominate." *In re Rail Freight Fuel Surcharge Antitrust Litig.*, 725 F.3d 244, 252-53 (D.C. Cir. 2013).

Second, the value of a consumer's PII also depends on characteristics specific to that consumer. [redacted] Olsen Dep. 190:20-25. Plaintiffs' expert Mitnick similarly opines [redacted] Dkt. 1260-16 ¶ 56. But Olsen [redacted] *See* Olsen Dep. 190:20–193:16. Plaintiffs thus gloss over "inherently individualized" damages issues, instead using impermissible averages, "divorced from any actual

[10] Remarkably, [redacted]. *See* Dkt 1260-7 at 6, Table 3 (calculating [redacted]); *id.* at 31, Table 10 [redacted]

proof of damages." *Broussard,* 155 F.3d at 342-43 (rejecting damages based on "abstract analysis of 'averages'" and the use of a "fictional 'typical franchisee operation'").

Compounding that error, the data stolen by Thompson varies greatly across the putative class. *See* Ex. H ¶ 100 (identifying 724 unique combinations of impacted data elements). Plaintiffs do not address this complexity, instead grouping "class damages" into just *four* basic categories, Dkt. 1260-7 at 31, Table 10. Further, Olsen ignores [redacted]. Ex. H ¶ 56. For instance, Olsen [redacted] Dkt. 1260-7 ¶ 48(e).

Finally, Plaintiffs fail to account for the facts that (i) much of the stolen data is outdated, given the length of the putative class period (2005-2019), and (ii) some of it is inaccurate. As Hitt notes, [redacted]." *See* Ex. H ¶¶ 75-77 & Exs. 1-3. Additionally, the stolen data may be worthless because Capital One (like any bank) routinely receives inaccurate application information. Plaintiffs cannot claim to have been injured by "unauthorized access" to information that is inaccurate or stale. And without examining each putative class member's circumstances—including a comparison of the stolen data to accurate and current data—it is impossible to ascertain the existence or extent of any injury. *See Gardner*, 2010 WL 11579028, at *4 (denying certification where plaintiffs did not show that class members "suffered from the same or similar injury" and "individualized inquiries would be required to prove both [liability] and the amount of damages due to each [class member]").

b. Plaintiffs' Market Value Theory Violates Wal-Mart.

The Supreme Court has rejected the concept of "Trial by Formula." *Wal-Mart*, 564 U.S. at 367. In *Wal-Mart*, the Court held that determining damages by calculating an "average backpay

award" and then applying that award "to the entire remaining class" to arrive at a total recovery figure violated the Rules Enabling Act and would deprive Wal-Mart of its right to litigate "defenses to individual claims." *Id.* Yet Olsen proposes the same approach here—*i.e.*, he "group[s] the exfiltrated PII into categories," "compar[es] them to the closest proxy of PII offered for sale on the Dark Web," "averag[es]" an unrepresentative sample of list prices for those proxies, and then "appl[ies]" those averages to assign damages to the putative class members. Dkt. 1260-7 ¶¶ 6, 48, 55; *see also* Dkt. 1432. A class may not be certified on that basis.

c. Individualized Inquiries Regarding Causation Predominate.

Finally, Plaintiffs fail to demonstrate that they can prove the Cyber Incident *caused* any Market Value injury with common, classwide proof. As the Court has already held, even if "Plaintiffs' PII has monetary value, Plaintiffs do not allege any facts explaining *how* their PII became less valuable as a result of the breach," as there "are no allegations that Plaintiffs attempted to sell their information and were refused a sale because of . . . their PII's prior exposure." Dkt. 879 at 29 (emphasis in original). Without that evidence—which would vary—Plaintiffs cannot show the Cyber Incident caused any putative class member to lose the market value of her data. *See* Ex. H ¶ 48 (Olsen has not "demonstrated that the [Cyber Incident] *caused* putative class members to lose the opportunity to sell their PII . . . or that they would be willing to do so in the first place"). "[I]ndividualized proof of damage causation" will thus "be essential to liability, destroying predominance." *Lienhart*, 255 F.3d at 149; *see also Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 697 (N.D. Cal 2019) (rejecting theory based on "unauthorized third parties[']"

access to personal information where plaintiff did not assert he would have charged "anyone to access comparable information").[11]

3. Plaintiffs' Disgorgement Theory of Damages Fails the Predominance Test.

Common questions will not predominate with respect to Plaintiffs' disgorgement theory, which they rely on for their breach of contract and unjust enrichment claims. *See* Mot. at 30 n.22 and 32 n.23. No Plaintiff can seek disgorgement. Nor is it possible to determine, using common evidence, whether or to what extent Capital One unjustly "retained" fraud savings from using Plaintiffs' or putative class member's application data.

a. No Plaintiff can seek disgorgement.

In Virginia, disgorgement is not an available remedy for breach of contract. *See* MSJ. And although disgorgement is available for an unjust enrichment claim, no Plaintiff has that claim. *See id.* Thus, Plaintiffs cannot seek disgorgement on behalf of the putative class.

b. Regardless, individualized issues would predominate on Plaintiffs' disgorgement theory.

Even if disgorgement were an available remedy, Plaintiffs have not met their burden of showing that common evidence can answer the question whether (and if so, to what extent) Capital One unjustly retained fraud savings from using any class member's application data. Plaintiffs rely entirely on the opinions of their expert, Gary Olsen, to try to show that this theory of recovery is susceptible to class treatment. But as explained below and in Capital One's motion to exclude Olsen's opinion, Dkt. 1432, Olsen's disgorgement model is fundamentally flawed and unreliable.

Olsen purports [redacted]. Specifically, Olsen opines

[11] In fact, [redacted]. Olsen Dep. 57:4-5; Ex. R, Rebuttal Expert Rep. of Gary Olsen ¶ 18; Dkt. 1386 at 13 n.7.

[redacted]. Dkt. 1260-7 ¶ 11. [redacted]

First, Plaintiffs' disgorgement theory assumes that Capital One benefited at the expense of all 98 million putative class members. That is incorrect. For example, during the 2015-2020 time period used in Olsen's calculation, Capital One's fraud models did not use data from any applications for Capital One branded cards (like the Capital One Venture card) submitted prior to 2014. *See* Kupiec Decl. ¶ 7, 11-12. But application data from as early as 2005 was stolen in the Cyber Incident. *See* Ex. E at 3. Thus, any putative class member who submitted an application for a Capital One branded card prior to 2014 conferred no benefit on Capital One under Olsen's theory, and that class member has no claim for disgorgement. Olsen fails to propose a "non-individualized means of identifying these uninjured class members." *In re Niaspan Antitrust Litig.*, 464 F. Supp. 3d 678, 720 (E.D. Pa. 2020).

Second, Olsen offers no method to determine whether any particular individual's data was successfully used to achieve any fraud savings (and if so, how much). Olsen's analysis does not identify the savings (if any) specifically attributable to Plaintiffs or any putative class member. Instead, Olsen simply [redacted]. Dkt. 1260-7 ¶ 71. Olsen cites no evidence to support this assumption, and in reality, determining whether and in what amount any given individual's data helped prevent fraud would require a person-by-person analysis. *See*

Kupiec Decl. ¶ 13 (stating that certain application data is more useful for fraud prevention than other application data). Because Plaintiffs "provided zero evidence as to how [they] will use common evidence to show which putative class members' [application data was successfully used for fraud prevention,]" Plaintiffs fail to meet Rule 23's predominance requirement. *Chudner v. Transunion Interactive, Inc.*, 2010 WL 5662966, at *1 n.1 (D. Del. Dec. 15, 2010) (denying certification of unjust enrichment claim).[12]

Third, even if Olsen could determine which putative class members' data was used to prevent fraud *and* the amount of fraud prevented, Olsen makes no attempt to address offsetting benefits they may have realized. Disgorgement damages are limited to the *net* benefit to the defendant after accounting for any benefits received by the plaintiff. *See* MSJ; *Kemp v. Cost Control Mktg. & Sales Mgmt. of Va., Inc.*, 790 F. Supp. 1275, 1277 (W.D. Va. 1992), *aff'd* 64 F.3d 920 (4th Cir. 1995) ("[R]estitution is excess of what purchasers paid over value of what they received."). Here, in exchange for providing their application, all putative class members received the benefit of having their applications considered. *See* Ex. H ¶ 121. As for fraud prevention specifically, many putative class members also benefited from Capital One's "robust fraud prevention program," including through reducing "the number of incidents of fraud and the number of false positives which inconvenience them." *Id.* ¶ 122.

For example, if a fraudster attempts to apply for a new Capital One card in a putative class member's name, Capital One's fraud models are designed to identify that fraud and prevent the account from being opened—thereby allowing the putative class member to avoid the time and

[12] The cases Plaintiffs rely on in support of certification of their unjust enrichment claim are inapposite. All of those cases involved bank overdraft fee practices and—unlike here—the putative class members affected by the defendants' allegedly improper schemes and their individual damages could be identified by basic calculations that were "merely ministerial in nature." *See In re Checking Account Overdraft Litig.*, 275 F.R.D. 666, 677 (S.D. Fla. 2011).

inconvenience of dealing with fraud. *See, e.g.,* Dkt. 971 ¶¶ 136-37 (alleging that identity theft can affect a victim's "ability to get … loans," and may "exact[] a severe emotional toll on its victims"). Assuming this benefit to the putative class member exceeds the $0.56 per year Capital One allegedly received from using her application data, she could recover no disgorgement damages. Olsen ignores these offsetting benefits, all of which would require individualized inquiry for each putative class member. And, importantly, these flaws in Olsen's opinions impact not only the amount of damages, but whether a putative class member is even entitled to disgorgement damages at all. *See Clay v. Am. Tobacco Co.*, 188 F.R.D. 483, 501 (S.D. Ill. 1999) ("[T]he defendants' liability for unjust enrichment to a particular plaintiff depends on the factual circumstances of the particular [transaction] at issue."). Olsen's opinions thus do not support certification of Plaintiffs' claims for breach of contract and unjust enrichment. *See In re Rail Freight*, 725 F.3d at 253 ("No damages model, no predominance, no class certification."); *see also Comcast*, 569 U.S. at 34-35.

B. Individual Issues Predominate as to Plaintiffs' Statutory Claims.

While Plaintiffs have done little to explain the specific theories of recovery for their statutory claims under California's UCL and CLRA, New York's GBL, and Washington's WCPA, it is clear those claims fail as a matter of law. *See* MSJ. Moreover, these claims are incapable of classwide adjudication under Rule 23. While each claim requires causation and injury,[13] Plaintiffs fail to identify *any* alleged injuries to support certification. *See* Mot. at 34-36. The Court should

[13] *See S.F. Residence Club, Inc. v. Amado*, 773 F. Supp. 2d 822, 833 (N.D. Cal. 2011) (injury required for UCL); *Kwikset Corp. v. Superior Ct.*, 246 P.3d 877, 887 (2011) (causation required for UCL); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111-13 (N.D. Cal. 2010) (causation and injury required for CLRA); *Fero v. Excellus Health Plan, Inc.*, 2020 WL 6866369 (W.D.N.Y. Nov. 23, 2020) (causation required for GBL); *Stutman v. Chem. Bank*, 731 N.E.2d 608, 612 (N.Y. 2000) (injury required for GBL); *Weidenhamer v. Expedia, Inc.*, 2015 WL 7157282, *14 (W.D. Wash. Nov. 13, 2015) (injury required for WCPA); *Panag v. Farmers Ins. Co. of Washington*, 204 P.3d 885, 889 (Wash. 2009) (causation required for WCPA).

therefore deny Plaintiffs' request for certification at the outset for failing to carry "the burden . . . of demonstrating satisfaction of the Rule 23 requirements." *Gariety*, 368 F.3d at 370.

Injury. If the Court nevertheless indulges Plaintiffs' threadbare request to certify these claims, it should conclude that none of the theories of harm on which the claims were allowed to survive Capital One's Motion to Dismiss are proper for representative litigation: **UCL** (Plaintiff Tada alleged she "spent money purchasing credit-monitoring and identity-theft protection services," Dkt. 879 at 56); **GBL** (Plaintiff Gershen alleged she "spent time and effort to regularly monitor [her] accounts to … mitigate potential harm," *id*. at 66); **WCPA** (Plaintiff Sharp alleged she "suffered identity theft and fraud in the form of unauthorized charges," and that she "spent time investigating the source of the fraud and unauthorized charges" and "regularly monitoring her accounts to detect fraudulent activity," *id*. at 73). None of these alleged harms is capable of being proven on a classwide basis, and Plaintiffs do not suggest otherwise. *See*, *e.g.*, *Weidenhamer*, 2015 WL 7157282, at *14 (denying class certification where determination of injury for purposes of WCPA claim was individualized issue). With respect to the **CLRA**, the Court did not specifically identify the alleged harm(s) upon which Plaintiffs stated a claim, *see* Dkt. 879 at 58-62, but none of the harms alleged by Plaintiff Tada—the proposed subclass representative—can be proven using common evidence, *see* Dkt. 971 ¶ 19. Moreover, Plaintiffs did not attempt to define the state subclasses to align with these alleged injuries, instead including "*[a]ll* persons in [the respective state] *whose PII was compromised in the Breach*"—or in the case of the CLRA Subclass, all such persons who *also* "sought or acquired a Capital One credit card for personal, family, or household purposes."[14] Mot. at 16-17 (emphasis added).

[14] Of course, determining whether a consumer applied for a card "for personal, family, or household purposes," as opposed to business or other purposes, would present yet another individualized issue (which cannot be cured by simply determining whether a card was a business

Causation. Plaintiffs' argument that they can prove the causation element of their statutory claims on a classwide basis due to a "presumption of reliance" is wrong. As an initial matter, Plaintiffs incorrectly assume "uniform misrepresentations" about Capital One's data security practices were made to all putative members of each state subclass. Mot. at 34. As discussed above, putative class members applied for credit through various channels over a 15-year period and were given different materials and disclosures regarding data security (if any). *See supra*, pps. 4-6. Thus, there are individualized questions surrounding what each class member saw and understood regarding Capital One's data security practices (if anything) when they applied for a credit card. For Plaintiffs' California statutory claims, "though reliance on a class-wide basis may be inferred based on materiality, such an inference cannot be made where the class members were not all exposed to the same alleged misrepresentations." *Torres v. Nissan N. Am. Inc.*, 2015 WL 5170539, at *5 (C.D. Cal. Sept. 1, 2015). Likewise, "while a [New York] plaintiff pursuing a GBL § 349 claim need not have relied on (or even necessarily have believed) the allegedly deceptive conduct, he or she must have at least been exposed to it." *Fero*, 2020 WL 6866369, at *9-10 (denying class certification in data breach case based on this issue). Lastly, Plaintiffs cannot avoid individualized causation inquiries under the WCPA for a *misrepresentation* claim, *Schnall v. AT&T Wireless Services, Inc.*, 259 P.3d 129, 137 (Wash. 2011), and to the extent they seek to rely on an *omission* theory (they do not say), it would still be plagued with predominance-defeating inquiries such as whether a putative class member suffered a requisite injury to "business or

---

card, as business cards can be used for personal purposes, and vice versa). Additionally, because an extension of credit is not covered by the CLRA, Plaintiffs must establish the existence of a service *ancillary* to the extension of credit. Dkt. 879 at 60-61. This too would require a highly individualized inquiry to determine the non-credit services each class member used, if any. *See Chittick v. Freedom Mortg. Corp.*, No. 1:18-cv-01034 (AJT/MSN) (E.D. Va. May 7, 2021), ECF No. 106 (denying class certification where determining the primary purpose of a loan and whether plaintiffs were subject to a safe harbor provision would require a "file-by-file" review).

property." *See Ambach v. French*, 216 P.3d 405, 408 (Wash. 2009) ("[T]he phrase 'business or property' in the [W]CPA is restrictive of other categories of injury and is 'used in the ordinary sense [to] denote[ ] a commercial venture or enterprise.") (quotation omitted).

C. Many Other Individualized Issues Foreclose Certification of Plaintiffs' Claims.

The Due Process Clause guarantees Capital One the right to raise "every available defense" to the claims asserted against it, including in a class action lawsuit. *See Lindsey v. Normet*, 405 U.S. 56, 66 (1972). A class cannot be certified if it would come at the expense of a defendant's ability to litigate its individual defenses. *See Wal-Mart,* 564 U.S. at 367; *Thorn*, 445 F.3d at 318. The Fourth Circuit strictly follows that principle, holding that when a claim depends on "facts peculiar to each plaintiff's case, class certification is erroneous" as a matter of law. *Broussard*, 155 F.3d at 342. With these principles in mind, multiple individual issues exist with respect to the elements of Plaintiffs' claims and the defenses that Capital One will assert.

1. <u>Plaintiffs' Breach of Contract Claim Fails to Satisfy Predominance.</u>

Breach of contract claims should not be certified where, as here, (a) the relevant contractual terms differ across the putative class, (b) class members would have to present individual proof on contract formation, or (c) resolving defenses would require facts specific to each class member. *See Broussard*, 155 F.3d at 340; *Fero*, 2020 WL 6866369, at *7, *11.

a. Material Changes to the Privacy Notice During the Putative Class Period Necessitate Individualized Inquiries.

Plaintiffs' breach of contract claims (express and implied) are premised on Capital One's Privacy Notice. *See* Mot. at 26-28. Plaintiffs assert that the same "standard form Privacy Notice" was "in effect throughout the class period." *Id.* at 26. Plaintiffs are wrong. As they acknowledge in a footnote, the Privacy Notice changed during the putative class period. *See id.* n.18. In 2010, Capital One began using a "Model Privacy Notice" promulgated by its regulators, which includes

a statement that "the bank's security measures 'comply with federal law.'" Mot. Ex. 3, Dkt. 1260-4, Expert Rep. of Brian Kelley ¶¶ 54-55. This is the language Plaintiffs have focused on for their breach of contract claim. *See* Mot. at 3. But before 2010, Capital One's Privacy Notice contained different language that did not refer to compliance with "federal law." *See* Dkt. 1260-32.

For example, Capital One's 2009 Privacy Notice states "[w]e maintain physical safeguards, such as secure areas in buildings; electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures to protect against ID theft." *See id.* at 1. There is no reference to "measures that comply with federal law" here, and this distinction matters. While Capital One disputes that the "federal law" language is contractually enforceable, Virginia courts "consider the words of [a] contract within the four corners of the instrument itself," "without adding terms." *Mathews v. PHH Mortg. Corp.*, 724 S.E.2d 196, 201 (Va. 2012). Plaintiffs' contention that the differences in Capital One's Privacy Notices are "immaterial" because "the relevant federal law" remained "the same" misses the point—a contractual obligation to "comply with federal law" is different from an obligation to, *e.g.*, use "electronic safeguards, such as passwords and encryption" (which Capital One indisputably did).

The legal effect of these changes is explained more fully in Capital One's MSJ, but the salient point for class certification is that individualized inquiries would be required to determine (i) when a given class member applied, (ii) which version of the Privacy Notice was then in effect, (iii) whether Capital One issued the class member a card, and (iv) if so, whether any updated version of the Privacy Notice—*i.e.*, a version including Plaintiffs' favored "comply with federal law" language—applies to that putative class member's information stolen in the Cyber Incident.[15]

[15] Plaintiffs cannot rescue their breach-of-contract claim by pointing to decisions generally holding that cases involving "form contracts" are appropriate for certification. *See* Mot. at 28 & n.21 (collecting cases). In the cases Plaintiffs cite, *liability* itself turned on the *interpretation* of a form

b. Individual Questions on Contract Formation Predominate as to the Applicant Class.

Because Applicants have no written agreement incorporating the Privacy Notice on which to base their breach-of-contract claim, individual inquiries are necessary to determine whether they can establish any contractual obligation—express or implied—concerning data security. Plaintiffs' assertion that the Privacy Notice is a "stand-alone" contract on which Applicants can sue is incorrect. *See* Mot. at 26-27; MSJ. The Privacy Notice itself "merely provides information—not commitments—regarding [Capital One's] use of information," *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 611 (9th Cir. 2020), and Applicants, who lack a written agreement, cannot enforce it. But even assuming the Privacy Notice could give rise to an obligation Applicants can enforce, individual inquiries would be required to determine if each putative class member (i) received the Privacy Notice when they applied and (ii) read or relied on it in submitting an application. *See Jones v. Peacock*, 591 S.E.2d 83, 87 (Va. 2004) (establishing a contract under Virginia law requires showing a "bilateral exchange, a meeting of the minds, and an understanding of obligations undertaken"); *Fero*, 2020 WL 6866369, at *11 (denying certification of contract claim in breach case where privacy notices were not uniformly provided to and read by class members). These determinations cannot be made with common proof.

First, there is no way to determine with common evidence whether a putative class member received the Privacy Notice at the time of her application. Capital One does not provide credit

---

contract common to all class members. *See, e.g.*, *In re TD Bank, N.A. Debit Card Overdraft Fee Litig.*, 325 F.R.D. 136, 155 (D.S.C. 2018) (overarching common issue was whether "uniform contract" permitted "Bank to impose overdraft fees"). But in this case, as explained above, whether Plaintiffs have suffered an injury *at all*, much less one caused by Capital One's conduct, requires individualized inquiries under any of Plaintiffs' injury theories. *See Manchester Oaks Homeowners Ass'n v. Batt*, 732 S.E.2d 690, 699 (Va. 2012) ("In a claim for breach of contract, proof of damages is an essential element and a plaintiff's failure to prove it requires that the action be dismissed."). Thus, even if the case "present[s] a common question of [breach], the issues of injury" and causation remain. *Windham v. Am. Brands, Inc.*, 565 F.2d 59, 66 (4th Cir. 1977).

card applicants with a copy of the Privacy Notice as a matter of course. Kottke Decl. ¶ 12. Instead, the materials given to an applicant depend on (i) which application channel that person used and (ii) any additional information the applicant sought out. *Id.* ¶¶ 10-11. Although some putative class members applied online (and thus *could* have clicked on the Privacy Notice), others applied in circumstances where the Privacy Notice would not have been provided—including in-person at a Capital One branch; at one of Capital One's partners' stores or with another card issuer; via mail solicitation; over the phone, and so on. *Id.* ¶¶ 20-22, 26-28, 31-32; *see also supra*, pps. 4-6.

Second, and more importantly, even those Applicants who had access to the Privacy Notice at the time they applied cannot be presumed to have read or relied on it.[16] And where there is "no evidence that [a plaintiff] was [even] aware of the existence of the contract," there can be "no mutual assent." *Giordano v. Atria Assisted Living*, 429 F. Supp. 2d 732, 736 (E.D. Va. 2006). There is no way to determine with common proof which putative class members read or relied on the Privacy Notice when applying for a credit card, which defeats predominance.[17]

c. Determining Which Putative Class Members Committed the First Material Breach Would Require Individualized Inquiries.

Virginia law is clear that "a party who commits the first [material] breach of a contract is not entitled to enforce the contract." *Horton v. Horton*, 487 S.E.2d 200, 203 (Va. 1997). A material breach is one that goes "to the root of the contract" and "deprive[s] the injured party of

[16] Illustrating this point, Plaintiff Behar and Member Plaintiff Baisden testified [redacted] Behar Dep. 35:15-17, Member Pl. Baisden Dep. 31:11-13, and Member Plaintiff Velez said, [redacted] Member Pl. Velez Dep. 55:21–25.

[17] The same issues plague Plaintiffs' implied contract theory, as such claims also require "mutuality of assent" and consideration of "the parties' conduct," *Spectra-4 LLP v. Uniwest Comm. Realty, Inc.*, 772 S.E.2d 290, 295 (Va. 2015), which cannot be shown with common proof.

the benefit that the party justifiably expected from the exchange." *RW Power Partners, L.P. v. Virginia Elec. & Power Co.*, 899 F. Supp. 1490, 1496 (E.D. Va. 1995).

Here, individual analyses would be required to determine whether each Cardholder class member defaulted and/or breached their respective Cardholder Agreements before the Cyber Incident. Taking the 54 active Member Plaintiffs and Representative Plaintiffs together, [redacted].[18] *See* Dkt. 387-6 at 4, Cardholder Agreement ("You will be in default if . . . you do not make any payment when it is due."). [redacted] *See* Sharp Dep. Ex. 5044. [redacted]. Member Pl. Velez Dep. 63:6-24; Ex. T at 25-28 ([redacted]). These are just examples, but accepting these examples as representative means millions of putative class members have breached their agreements with Capital One, too.

Relatedly, certification of Plaintiffs' breach of contract claim is improper because there is no common method to adjudicate Capital One's defenses of setoff and recoupment. Under these doctrines, a defendant has the right to reduce (or extinguish) a plaintiff's monetary claim due to a claim the defendant has against that plaintiff. *See F.D.I.C. v. Marine Midland Realty Credit Corp.*, 17 F.3d 715, 722 (4th Cir. 1994). Capital One is entitled to litigate and offset any amounts owing on each Plaintiff's and class member's account—e.g., [redacted], which would exceed her requested recovery here. Sharp Dep. Ex. 5044; *see*

[18] *See* Ex. S ([redacted]); Ex. T at 25-28; Tada Dep. Ex. 5058; Sharp Dep. Ex. 5044; Member Pl. DeLeon Dep. 54:7-19 ([redacted]).

In re Digital Music Antitrust Litig., 321 F.R.D. 64, 88 (S.D.N.Y. 2017) (denying class certification, in part, because "class members will be subject to counterclaims for a setoff").

Plaintiffs have offered no common method by which to address these individualized defenses. To the contrary, resolving Capital One's first-material-breach and setoff/recoupment defenses would devolve into millions of mini-trials incapable of classwide resolution.

2. Plaintiffs' Unjust Enrichment Claim Fails to Satisfy Predominance.

Even if Plaintiffs had a viable method of determining disgorgement damages on a classwide basis, their unjust enrichment claim would still fail Rule 23's predominance test because of other inherently individualized issues concerning causation *and* the statute of limitations. Notably, Plaintiffs cite no case, nor has research revealed any, where a court certified a Rule 23(b)(3) class for an unjust enrichment claim in a data breach case. "[C]ommon questions will rarely, if ever, predominate an unjust enrichment claim, the resolution of which turns on individualized facts." *Vega v. T-Mobile USA, Inc.*, 564 F.3d 1256, 1274 (11th Cir. 2009).

a. Causation Cannot Be Established with Common Proof.

Under Plaintiffs' unjust enrichment theory, every Plaintiff and putative class member must show that their data "would not have been transferred to and entrusted with" Capital One—*i.e.*, they would not have applied for a credit card—"[b]ut for [Capital One's] willingness and commitment to maintain its privacy and confidentiality." Dkt. 971 ¶ 183; *see* Dkt. 1260-7 ¶ 19 (premising disgorgement opinion on assumption that, "[h]ad each of the Representative Plaintiffs known that Capital One's data security measures were inadequate to safeguard customers' PII, they would not have provided their PII to Capital One"); *see also Marsteller v. ECS Fed., Inc.*, 2013 WL 4781786, at *10 (E.D. Va. Sept. 5, 2013) (unjust enrichment requires "causal relationship" between "allegedly wrongful activities" and benefit retained by defendant). Yet Plaintiffs offer no common method—and there is none—by which to prove that every putative

class member would have refrained from applying for a credit card had he or she known about Capital One's allegedly deficient cybersecurity practices.

Nor can the Court simply take Plaintiffs' word for it on this point. Even after the Cyber Incident was announced, [redacted]." Ex. H ¶ 139. Moreover, Plaintiffs' conduct following the Cyber Incident suggests that they might have applied *even if* they had known of the alleged deficiencies. [redacted] Sharp Dep. 68:4-12. [redacted] *See*, *e.g.*, Behar Dep. 65:3-21; Edmondson Dep. 85:12-86:10; Zielicke Dep. 78:18-22. Likewise, even if Capital One's allegedly deficient cybersecurity had been well known before the Cyber Incident, some putative class members may have determined that the benefits of applying simply outweighed any risks. *See* Ex. H ¶¶ 140-143. In short, the "specific evidence" required to determine whether any class member would have applied for a card had she known of Capital One's alleged deficiencies "is incompatible with representative litigation." *Grandalski v. Quest Diagnostics Inc.*, 767 F.3d 175, 185 (3d Cir. 2014) (affirming denial of certification of unjust enrichment claim where "individual inquiries would be required to determine whether an alleged overbilling constituted unjust enrichment for each class member").

b. Determining Which Putative Class Members Are Barred by the Statute of Limitations Would Require Individualized Inquiries.

Plaintiffs also fail to offer a common method to determine which putative class members' unjust enrichment claims are barred by Virginia's three-year statute of limitations. *See* Va. Code Ann. § 8.01-246; Dkt. 1296 at 42. Plaintiffs bear the burden of "affirmatively [showing] that

resolution of th[is] statute of limitations defense on its merits may be accomplished on a class-wide basis." *Thorn*, 445 F.3d at 321. They have not carried that burden.

Plaintiffs' unjust enrichment claim is not "tethered to the [Cyber Incident]," *see* Dkt. 1298, May 7, 2021 Hr'g Tr. 16:11-17:4; *see also id.* 5:7-13, 6:8-21, but rather is based on Capital One "benefiting" from their information without protecting it, which Plaintiffs say began when Capital One moved to the cloud in 2015. *See* Mot. Ex. 4, Dkt. 1260-5, Expert Rep. of Stuart Madnick at 18 (stating that relevant misconfiguration was implemented in Capital One's cloud environment "[i]n or around 2015"); Dkt. 1260-7, Sched. 14.1 (calculating disgorgement damages from January 1, 2015).[19] Thus, determining which individuals are barred from asserting an unjust enrichment claim would require individualized inquiries concerning (among other things): (1) when they provided data to Capital One;[20] (2) when Capital One migrated their data to the cloud; and (3) when (if ever) Capital One benefited from using that data for fraud prevention. Plaintiffs fail to explain how these questions can be answered on a classwide basis using common evidence—and they cannot be. Nor can Plaintiffs avoid this issue by invoking the discovery rule: "[t]he statute of limitations for unjust enrichment begins to run at the time the unjust enrichment occurred . . . not when a party 'knew or should have known' of the unjust enrichment." *Tao of Sys. Integration, Inc. v. Analytical Servs. & Materials, Inc.*, 299 F. Supp. 2d 565, 576 (E.D. Va. 2004).

[19] Under Plaintiffs' recast unjust enrichment theory, the classes they seek to represent are not properly defined because the population of consumers whose data Capital One retained since moving to the cloud in 2015 is not coextensive with the putative class of consumers allegedly impacted by the Cyber Incident. This disconnect between the classes Plaintiffs purport to represent and the claim they ask the Court to certify further highlights their inadequacy under Rule 23(a)(4).

[20] Notably, the statute of limitations has run for half of the Plaintiffs' unjust enrichment claims. Plaintiffs Edmondson, Hausauer, and Tada all applied before January 1, 2015 (*see* Exs. A, MM, NN), so their claims accrued on January 1, 2015. Plaintiff Gershen's claim also accrued no later than January 31, 2015 because she applied in January 2015. *See* Ex. OO. Accordingly, all of these Plaintiffs' unjust enrichment claims were extinguished no later than January 31, 2018.

3. Millions of Putative Class Members are Subject to Affirmative Defenses That Require Individualized Inquiries.

The Fourth Circuit has flatly held "that when [a] defendant's affirmative defenses … may depend on facts peculiar to each plaintiff's case," predominance is not satisfied. *Broussard*, 155 F.3d at 342. Notably, the *plaintiff* bears the burden of proving that the presence of individualized defenses does not defeat class certification. *Thorn*, 445 F.3d at 318. Here, Capital One's affirmative defenses require extensive individualized inquiries.

a. Capital One's Limitation of Liability Defense Cannot Be Resolved With Common Proof.

Several Plaintiffs—namely, Gershen, Hausauer, Sharp, Spacek, and Tada—submitted online applications for Capital One credit cards, as did millions of putative class members. Kottke Decl. ¶ 17. Any claims "arising out of" Plaintiffs' provision of information in these online applications are barred by a limitation of liability clause contained in the Terms and Conditions of Capital One's website, *see* MSJ, and determining whether this defense applies to the putative class members' claims would require individualized assessments concerning, *e.g.*, the specific way in which each class member submitted their application data to Capital One.[21] Notably, limitation of liability clauses like Capital One's are enforceable in Virginia. *See Hiett v. Lake Barcroft Comm. Ass'n,* 418 S.E.2d 894, 896 (Va. 1992). And courts have enforced similar clauses to preclude claims arising from data breaches. *See Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (enforcing limitation of liability clause in Facebook's terms of service to preclude

[21] The limitation of liability clause provides that: "***IN NO EVENT SHALL CAPITAL ONE BE LIABLE FOR . . . ANY DAMAGES WHATSOEVER***, … ***WITHOUT REGARD TO THE FORM OF ANY ACTION, INCLUDING BUT NOT LIMITED TO CONTRACT AND TORT ACTIONS*** (INCLUDING LIBEL), ***ARISING OUT OF OR IN CONNECTION WITH THE USE***, COPYING OR DISPLAY ***OF, OR THE INTERACTION OR ANY OF FORM OF COMMUNICATION WITH, THE SITE*** AND THE INFORMATION CONTAINED AT THE SITE." Ex. U (July 2015 Terms and Conditions) (emphasis added).

contractual and quasi-contractual claims, among others). Capital One is therefore entitled to assert this defense as to each online applicant class member. *See Lindsey,* 405 U.S. at 66.

b. Capital One's Failure to Mitigate and Contributory Negligence Defenses Cannot Be Resolved With Common Proof.

Virginia courts "recognize[] the obligation of an injured party to mitigate damages" in the context of both tort and contract claims, and a plaintiff's failure to do so entitles the defendant to offset any damages it may owe. *See Forbes v. Rapp*, 611 S.E.2d 592, 595 (Va. 2005); *Monahan v. Obici Med. Mgmt. Servs., Inc.*, 628 S.E.2d 330, 336 (Va. 2006). Similarly, contributory negligence is a complete defense to negligence claims under Virginia law and applies where a plaintiff fails to take reasonable precautions; the "essence of contributory negligence is carelessness." *Ponirakis v. Choi*, 546 S.E.2d 707, 710-11 (Va. 2001). There is no evidence that Thompson disseminated the stolen information, but assuming *arguendo* that she did, then Capital One is entitled to raise these defenses against the putative class members to whom they apply.

The evidence developed so far suggests these defenses are viable. For example, [redacted], Ex. H ¶ 111, [redacted] *See* Mot. Ex. 18, Dkt. 1260-19, Gershen Resp. to Interrog. No. 5 at 13; Mot. Ex. 22, Dkt. 1260-23, Zielicke Resp. to Interrog. No. 5 at 13. [redacted]. *See* Ex. H. ¶ 111. Moreover, many putative class members—like the Plaintiffs discussed above—have likely disclosed their information publicly (*e.g.*, on social media). Capital One therefore has a due process right—just as it would in a trial involving an individual plaintiff—to develop evidence to support its defenses that putative class members failed to mitigate their damages or were contributorily negligent.

Plaintiffs cannot deprive Capital One of its right to assert these defenses, *see Lindsey*, 405 U.S. 56, and resolving them would require individual inquiry, defeating predominance.[22]

IV. PLAINTIFFS' EMPHASIS ON NOMINAL DAMAGES CONFIRMS THAT A CLASS ACTION IS AN INFERIOR METHOD OF ADJUDICATION.

After failing to find evidence of actual harm caused by the Cyber Incident, Plaintiffs have shifted their focus to seeking nominal damages for their breach-of-contract claim. But for several reasons, certifying a "nominal damages class" would violate Rule 23 and would not be a superior method for adjudicating Plaintiffs' proposed nationwide breach of contract claim.

First, Plaintiffs are wrong that the availability of nominal damages for a breach of contract relieves them of the requirement to individually prove causation and actual injury. *See Filak v. George*, 594 S.E.2d 610, 614 (Va. 2004) ("injury or damage to the plaintiff" is essential element of contract claim); *Bailey v. Potter*, 2006 WL 1582410, at *4 (E.D. Va. June 5, 2006) (potential for nominal damages does not "eviscerate the 'consequential injury or damage' element of a claim for breach of contract"); *see also* MSJ. Thus, even if Plaintiffs elect to pursue only nominal damages, each Plaintiff and putative class member must still present individualized evidence proving that Capital One's alleged breach of the Privacy Notice injured them. For the reasons set out above, individualized inquiries on causation and injury would be "unwieldy and unmanageable as a class action." *Kelecseny v. Chevron, U.S.A., Inc.*, 262 F.R.D. 660, 677 (S.D. Fla. 2009).

Second, Plaintiffs' suggestion that they could obtain nominal damages as a baseline classwide recovery and then also seek other forms of contract damages, *see* Mot. at 29-30, is also

[22] In addition to failing the predominance test, Plaintiffs cannot satisfy Rule 23's superiority requirement, which focuses on the feasibility of trying the case as a class action. *See* Advisory Comm. Notes to 2003 Am. of Fed. R. Civ. P. 23 ("A critical need is to determine how the case will be tried."). Due to the overwhelming number of individualized issues present in this case, a trial of the claims Plaintiffs seek to certify would be both unwieldy and completely unmanageable.

wrong. "[N]ominal damages are only available under Virginia law when compensatory damages are unwarranted or unprovable." *JTH Tax, Inc. v. Aime*, 984 F.3d 284, 294 (4th Cir. 2021) (vacating award of nominal damages made in addition to other contract damages). So, even if Plaintiffs succeeded in proving a breach of contract and obtained a nominal damages award, they (and the putative class) would then be foreclosed from pursuing the actual damages they allege in the Complaint.[23] Dkt. 971 ¶ 140. Abandoning alleged class damages for a nominal recovery does not satisfy Rule 23's superiority requirement. "This is Rule 23 in reverse," with Plaintiffs "assum[ing] that a class action is superior, and then fram[ing] the question of damages so that it smooths over all factual variation." *Amador v. Baca*, 299 F.R.D. 618, 634 (C.D. Cal. 2014), *rev'd in part on other grounds*, 2014 WL 10044904.

Third, Plaintiffs' argument that a nominal-damages-only class satisfies superiority is premised on a fundamentally mistaken view of the law. Plaintiffs apparently intend to argue that if they can prove Capital One breached the Privacy Notice, *each* of the 98 million putative class members should get at least $1, and as much as $100—*i.e.*, an award between $98 million and $9.8 billion. *See*, *e.g.*, Dkt. 1229, Mar. 9, 2021 Hr'g Tr. at 12:12-20 (suggesting *each* putative class member could recover up to $100 in nominal damages). That position is nonsensical. An award of $98 million or more would clearly not qualify as "nominal damages," which Virginia

[23] The Court should consider Plaintiffs' motivations for prioritizing nominal damages over the actual damages they claim the putative class suffered. *See* Dkt. 971 ¶ 140. Perhaps Plaintiffs simply recognize that they suffered no compensable damages as a result of the Cyber Incident (Capital One agrees). Or it could be a product of Plaintiffs' singular focus on obtaining class certification, which calls into question their adequacy as class representatives. *See Standard Fire Ins. Co. v. Knowles*, 568 U.S. 588, 594 (2013) (suggesting that "a court might find that Knowles is an inadequate representative due to the artificial cap he purports to impose on the class' recovery"). At a minimum, Plaintiffs' pretrial election of nominal damages would conflict with the interests of any putative class members who believe (albeit incorrectly) that the Cyber Incident caused them actual damages. *Sharp Farms v. Speaks*, 917 F.3d 276, 297 (4th Cir. 2019).

courts uniformly describe as "token" or "trivial." *See Kerns v. Wells Fargo Bank, N.A.*, 818 S.E.2d 779, 786 (Va. 2018) (quoting Sinclair on Virginia Remedies § 1-1, at 1-5 (5th ed. 2016)); *Rickman v. Commonwealth*, 808 S.E.2d 395, 396 n.1 (Va. 2017) ("Nominal damages consist of a trivial amount of money[.]").

Courts rarely award nominal damages in class actions, but when they do, they ensure that the award does not exceed a trivial amount, typically by awarding nominal damages to the class as a whole or only to the class representatives. The Fourth Circuit has endorsed that approach. *See Norwood v. Bain*, 166 F.3d 243, 245 (4th Cir. 1999) (*en banc/per curiam*) (remanding with instructions to enter judgment "that includes an award of nominal damages to the plaintiff class against [defendants] not exceeding $1.00"). Many other courts have, too. *See*, *e.g.*, *Madison Cty. Jail Inmates v. Thompson*, 773 F.2d 834, 836, 845 (7th Cir. 1985) (holding that nominal damages of $1 to each of two subclasses—not to each class member—was appropriate); *Davenport v. DeRobertis*, 653 F. Supp. 649, 652 (N.D. Ill. 1987) (awarding one dollar in nominal damages to each named plaintiff); *Alexander v. Polk*, 572 F. Supp. 605, 623 (E.D. Pa. 1983) (awarding $1.00 in nominal damages to the class), *rev'd in part on other grounds*, 750 F.2d 250 (3d Cir. 1984).

Nor do the cases Plaintiffs cite support the conclusion that nominal damages can turn their no-injury contract claim into a stratospheric recovery. Those cases rely on the Ninth Circuit's decision in *Cummings v. Connell*, which expressly acknowledged that its holding ran contrary to the Fourth Circuit's decision in *Norwood.* *See* 402 F.3d 936, 943 (9th Cir. 2005). In fact, *Opperman v. Path, Inc.*—the only case Plaintiffs cite not involving constitutional rights violations—does not even address whether nominal damages would be awarded to the class (or class representatives) or to each individual class member. 2016 WL 3844326 at *16 (N.D. Cal. July 15, 2016) (holding only that "the nominal damages claims of [the] Intrusion Upload Subclass

can be determined on a classwide basis"). The Court should deny Plaintiffs' request to certify a nationwide nominal-damages-only breach of contract claim.[24]

V. THE COURT SHOULD NOT CERTIFY A RULE 23(B)(2) CLASS.

Plaintiffs also seek to certify a Rule 23(b)(2) class for "declaratory" and "injunctive" relief requiring Capital One to implement "security controls needed to protect class members' PII now and in the future." Mot. at 39. Plaintiffs' request should be denied.

First, Plaintiffs lack standing because they are not at an imminent risk of suffering harm from another similar data breach at Capital One. *See* Dkt. 1386. "Having failed to allege a real and imminent threat of future [harm], [Plaintiffs] do not have standing to pursue a Rule 23(b)(2) class action for injunctive relief." *Drayton v. W. Auto Supply Co.*, 2002 WL 32508918, at *5 (11th Cir. Mar. 11, 2002).

Second, even if Plaintiffs had standing, a Rule 23(b)(2) class is inappropriate because Plaintiffs seek primarily monetary relief. *Berry v. Schulman*, 807 F.3d 600, 609 (4th Cir. 2015) ("Where monetary relief predominates, Rule 23(b)(2) certification is inappropriate."). Plaintiffs suggest that this basic principle does not apply because they seek to certify both a 23(b)(3) *and* a 23(b)(2) class. Mot. at 38. But courts routinely deny certification of Rule 23(b)(2) classes when the thrust of the plaintiff's case is for monetary damages, regardless of whether the plaintiff requests a separate class for injunctive relief alone. *See, e.g.*, *McGlenn*, 2021 WL 165121, at *7 (denying 23(b)(2) class in data breach case because "the allegations and arguments indicate that

[24] Additionally, because Plaintiffs cannot show that any putative class members were injured due to Capital One's alleged breach of contract, a $98 million or $9.8 billion award "would be enormous and completely out of proportion to any harm suffered" and would undoubtedly raise due process concerns. *London v. Wal-Mart Stores, Inc.*, 340 F.3d 1246, 1255 n.5 (11th Cir. 2003); *In re Trans Union Corp. Privacy Litig.*, 211 F.R.D. 328, 350-51 (D. Ill. 2002) (holding that "a class action is not the superior method" where certification "could result in statutory minimum damages of over $19 billion, which [would be] grossly disproportionate to any actual damage").

Plaintiff's main goal is monetary damages"); *Kottaras v. Whole Foods Mkt., Inc.*, 281 F.R.D. 16, 27 (D.D.C. 2012) (similar).

Third, the requested injunctive relief is inappropriate and unnecessary. "A mandatory injunction imposes significant burdens on the defendant and requires careful consideration of the intrusiveness of the ordered act, as well as the difficulties . . . in supervising the enjoined party's compliance." *Kartman v. State Farm Mut. Auto. Ins.*, 634 F.3d 883, 892 (7th Cir. 2011). Plaintiffs, however, ask this Court to order Capital One to monitor criminal dark web sites and marketplaces, and potentially engage in dealings with criminals. *See, e.g.*, Mot. at 39 (injunction would include "[m]aintaining a consistent and continuous effort to search for the breached data on dark web marketplaces" and "[e]nsuring that all breached data has been discovered and destroyed"). The Court should decline that problematic request for many reasons, chief among them that scouring the dark web for data that was *never disseminated beyond Paige Thompson* would be a waste of resources. The balance of Plaintiffs' requested relief—concerning Capital One's own data privacy practices—is likewise unnecessary because Capital One has already fully remediated the issues that led to the Cyber Incident. *See* Dkt. 1348-2. Moreover, many of the measures Plaintiffs seek to impose, such as deleting data from Capital One's secured systems, are unrelated to the vulnerabilities that led to the Cyber Incident. *See Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1140 (9th Cir. 2009) ("Injunctive relief . . . must be tailored to remedy the specific harm alleged.").[25]

VI. THE COURT SHOULD DENY ISSUE CERTIFICATION UNDER RULE 23(C).

"[I]n the alternative" to their request for certification under Rule 23(b)(2) and (b)(3), Plaintiffs ask the Court to certify "issues-based classes—*e.g.*, for duty and breach as to both [their]

[25] Capital One's remedial efforts distinguish this case from the Rule 23(b)(2) ruling in *Adkins*—particularly because there, unlike here, the court noted that Facebook had caused "repetitive losses of users' privacy." 424 F. Supp. 3d at 686. No such facts are present here.

negligence and contract claims"—under Rule 23(c)(4). Mot. at 39-40. The Court should reject that proposal. To begin, "issue certification is not appropriate where *the determination of liability itself* requires an individualized inquiry." 1 McLaughlin on Class Actions § 4:43 (17th ed. 2020) (emphasis added). Yet, the issues left out of Plaintiffs' proposed 23(c)(4) classes—causation and injury—are essential elements of *liability* for their negligence and contract claims. *See* MSJ.

Moreover, issue certification is appropriate "only where resolution of the particular common issues would materially advance the disposition of the litigation as a whole," *Rahman v. Mott's LLP*, 2014 WL 6815779, at *9 (N.D. Cal. Dec. 3, 2014), and courts decline "to certify [issue] classes where the prevalence of individual issues is such that limited class certification would do little to increase the efficiency of the litigation." *Naparala v. Pella Corp.*, 2016 WL 3125473, at *14 (D.S.C. June 3, 2016). Here, the certification of "issues classes" as to the elements of duty and breach would *not* increase the efficiency of the litigation. Plaintiffs' case is riddled with critical liability issues concerning causation and injury, all of which require individual scrutiny. *See supra*, pps. 18-32. Plaintiffs assert that "a class-wide determination of the issues most burdensome to prove" is warranted, Mot. at 40, but the "most burdensome" issues are those this Court would be left with if the proposed issues classes were certified. *See Rahman*, 2014 WL 6815779, at *9 ("[A]llowing myriad individual damages claims to go forward hardly seems like a reasonable or efficient alternative.").

CONCLUSION

For these reasons, the Court should deny Plaintiffs' motion for class certification.

Dated: May 28, 2021

Respectfully submitted,

/s/
David L. Balser (*pro hac vice*)
S. Stewart Haskins II (*pro hac vice*)
Susan M. Clare (*pro hac vice*)
John C. Toro (*pro hac vice*)

Kevin J. O'Brien (VSB No. 78886)
Robert D. Griest (*pro hac vice*)
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, GA 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
sclare@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
TROUTMAN PEPPER HAMILTON SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Tel.: (804) 697-1200
Fax: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
S. Mohsin Reza (VSB No. 75347)
TROUTMAN PEPPER HAMILTON SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Tel.: (202) 274-1932
Fax: (202) 274-2994
mary.zinsner@troutman.com
mohsin.reza@troutman.com

Counsel for Capital One Defendants

CERTIFICATE OF SERVICE

I hereby certify that on May 28, 2021, I caused the foregoing document to be filed with the Clerk of Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/
David L. Balser

Counsel for Capital One Defendants

APPENDIX A: Prior Breaches, Exposures, and Misuses of Plaintiffs' Information

Plaintiff	Prior Data Breach(es)
Behar	[redacted]
Edmondson	[redacted]
Gershen	[redacted]
Hausauer	[redacted]
Sharp	[redacted]
Spacek	[redacted]
Tada	[redacted]
Zielicke	[redacted]

Plaintiff	Prior Identity Frauds
Gershen	[redacted]
Hausauer	[redacted]
Spacek	[redacted]
Tada	[redacted]